Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A cryptographic system, ~~with at least one server and any number of clients, including none, the cryptographic system further~~ comprising:

at least one server;

any number of clients;

at least one application located on one of the at least one server, each capable of engaging in a context-free multi-part communication session with any of the clients;

a key repository process on one of the at least one server, the key repository process configured to validate and record authorizations of specific programs to access one or more than one set of symmetric keys, wherein each of the at least one application is configured to query the key repository process for one or more than one set of symmetric keys, and the key repository process further configured, in response to the query from a particular instance of the at least one application, to provide the requested one or more than one set of symmetric keys to the particular instance of the at least one application but only if the key repository process authenticates the particular instance of the at least one application as being pre-authorized to receive the requested one or more than one set of symmetric keys;

~~wherein,~~ the particular instance of the at least one application can utilize the one or more than one set of symmetric keys for securely off-loading sensitive information in any intermediate part of the context-free multi-part communication session; and

the key repository process includes a database for storing the one or more than one set of symmetric keys, each set of symmetric keys including an integrity key for ensuring the integrity of information stored in the database and a protection

key configured to protect sensitive information on the database, the database storing there within operator entries used to retain the value of the integrity key and owner entries used to retain a share of the protection key.

2. (Currently amended) The cryptographic system as in claim 1, wherein the sensitive information in an intermediate part is securely off-loaded to ~~a~~ the database.

3. (Original) The cryptographic system as in claim 1, wherein the sensitive information in an intermediate part is securely off-loaded as a cookie to an intended one of the clients that returns the cookie within a next part of the context-free multi-part communication session.

4. (Original) The cryptographic system as in claim 1, wherein the key repository process maintains one set of symmetric keys for all of the at least one application.

5. (Original) The cryptographic system as in claim 1, wherein the key repository process maintains a distinct set of symmetric keys for each one of the at least one application.

6. (Original) The cryptographic system as in claim 1, wherein the text-free multi-part communication session is conducted using a hypertext transfer protocol.

7. (Original) The cryptographic system as in claim 1, wherein both the at least one application and the at least one server utilize one of a hypertext markup language, a standard generalized markup language, and an extensible markup language.

8. (Original) The cryptographic system as in claim 1, wherein the securely off-loaded sensitive information can be then accessed by any one of the at least one application engaging in the context-free multi-part communication session.

9. (Original) The cryptographic system as in claim 1, wherein the securely off-loaded sensitive information is encrypted.

10. (Original) The cryptographic system as in claim 1, wherein the sensitive data is securely off-loaded to a working memory in a server to enable a single server process instance to service all communications between the at least one application and the server.

11. (Original) The cryptographic system as in claim 1, wherein the at least one application includes instances of the same application.

12. (Currently amended) The cryptographic system as in claim 1, wherein the key Rrepository process is a process pair.

13. (Currently amended) A method for secure context-free multi-part communication in a computer system with a server and any number of clients, including none, the method comprising:

instantiating at least one application on the server, each capable of engaging in a context-free multi-part communication session with any of the clients;

instantiating a key repository process on the server, so that

the key repository process validates and records authorizations of specific applications to access one or more than one set of symmetric keys, wherein each of the at least one application is configured to query the key repository process for one or more than one set of symmetric keys, and

in response to the query from a particular instance of the at least one application, the key repository process provides the requested one or more

than one set of symmetric keys to the particular instance of the at least one application but only if the key repository process authenticates the particular instance of the at least one application as being pre-authorized to obtain the requested one or more than one set of symmetric keys;

wherein, the particular instance of the at least one application utilizes the one or more than one set of symmetric keys for securely off-loading sensitive information in any intermediate part of the context-free multi-part communication session and the key repository process includes a database for storing the one or more than one set of symmetric keys, each set of symmetric keys including an integrity key for ensuring the integrity of information stored in the database and a protection key configured to protect sensitive information on the database, the database storing there within operator entries used to retain the value of the integrity key and owner entries used to retain a share of the protection key.

14. (New) A server, comprising:

a key repository, the key repository configured to validate and record authorizations of specific programs to access one or more than one set of symmetric keys, wherein an application is configured to query the key repository for one or more than one set of symmetric keys, and the key repository responsive to the query from the application, provides the requested one or more than one set of symmetric keys to the application but only if the key repository authenticates the application as being pre-authorized to receive the requested one or more than one set of symmetric keys, the application can utilize the one or more than one set of symmetric keys for securely off-loading sensitive information; and

a database for storing the one or more than one set of symmetric keys, each set of symmetric keys including an integrity key for ensuring the integrity of information stored in the database and a protection key configured to protect sensitive information on the database, the database storing there within operator entries used to retain the value of the integrity key and owner entries used to retain a share of the protection key.

15. (New) A server as defined in claim 14, wherein the server utilizes one of a hypertext markup language, a standard generalized markup language, and an extensible markup language.

16. (New) A server as defined in claim 14, wherein the sensitive information in an intermediate part is securely off-loaded as a cookie.

17. (New) A server as defined in claim 14, wherein the securely off-loaded sensitive information is encrypted.

18. (New) A method for establishing a secure communication session by a client, the method comprising:

establishing a context-free multi-part communication session with a server; and

causing in response to a query by the client of an application, a key repository process to be configured to validate and record authorizations of specific programs to access one or more than one set of symmetric keys, wherein the application is configured to query the key repository process for one or more than one set of symmetric keys, and the key repository process is further configured, in response to the query from the application, to provide the requested one or more than one set of symmetric keys to the application but only if the key repository process authenticates the particular application as being pre-authorized to receive the requested one or more than one set of symmetric keys; the key repository process including a database for storing the one or more than one set of symmetric keys, each set of symmetric keys including an integrity key for ensuring the integrity of information stored in the database and a protection key configured to protect sensitive information on the database, the database storing there within operator entries used to retain the value of the integrity key and owner entries used to retain a share of the protection key.